(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁷: H04L 9/06

(21) International Application Number:
PCT/IB2004/050850

(22) International Filing Date: 7 June 2004 (07.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03101719.7   12 June 2003 (12.06.2003)   EP

(71) Applicant (for DE only): PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant (for all designated States except US): KONINKLIJKE PHILIPS ELECTRONICS N. V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants (for US only): ROTTSCHÄFER, Thomas [DE/DE]; c/o Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

WAGNER, Mathias [DE/DE]; c/o Philips Intellectual Property &, Standards GmbH Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: MEYER, Michael; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

(54) Title: PROCESSOR FOR ENCRYPTING AND/OR DECRYPTING DATA AND METHOD OF ENCRYPTING AND/OR DECRYPTING DATA USING SUCH A PROCESSOR
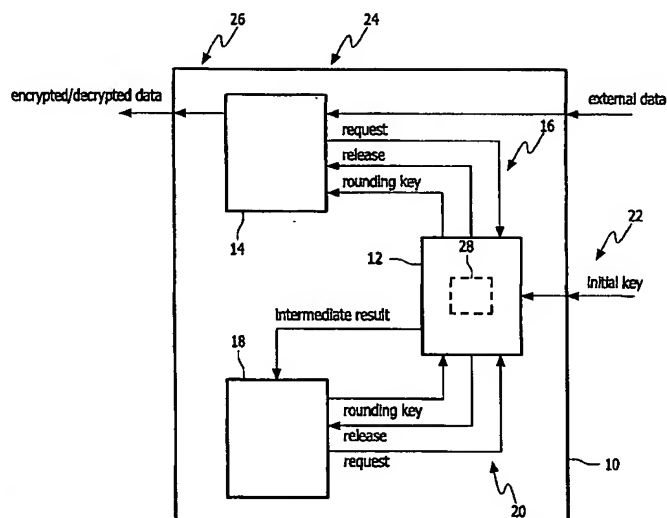
(57) Abstract: In order to provide a processor for encrypting and/or decrypting data and a method of encrypting and/or decrypting data using such a processor, which are characterized by a lower storage requirement and greater safety against attacks on the rounding key generation than previously known and which are preferably embodied as, respectively, an AES coprocessor and a method of AES calculation, it is provided that a control device (12) is connected to at least one encryption/decryption means (14) via at least one communication means (16), the control device (12) is connected to at least one rounding key generation means (18) via at least one further communication means (20), the control device (12) has at least one external key input (22), the at least one encryption/decryption means (14) has at least one external data input (24) and at least one external data output (26), and the at least one encryption/decryption means (14) and the at least one rounding key generation means (18) are decoupled from one another. The method according to the invention provides that at least one initial key is read into a control device, external data are read into at least one encryption/decryption means, at least one data word needed to calculate at least one rounding key is read from at least one storage means of the control device and transferred to at least one rounding key generation means, at least one rounding key is calculated recursively on the basis of the at least one data word by means of the at least one rounding key generation means, transferred to the control device and stored in the at least one storage means, the at least one rounding key is transferred to the at least one encryption/decryption means, the external data are encrypted or decrypted by means of the at least one encryption/decryption means using the at least one rounding key and the encrypted or decrypted data are made available at least one external data output, and these steps are repeated as often as necessary to encrypt or decrypt a set of external data.

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.